# IP Address Allocation, Resolution

Cabrillo College

CIS 81 and CST 311

Rick Graziani

Cabrillo College

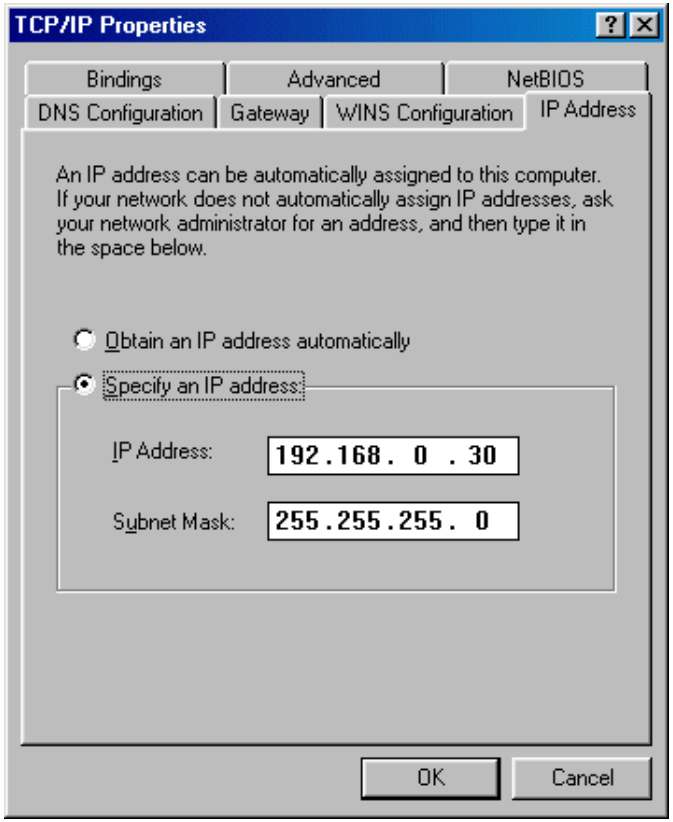
Spring 2006

# Address Allocation

# IP Addressing



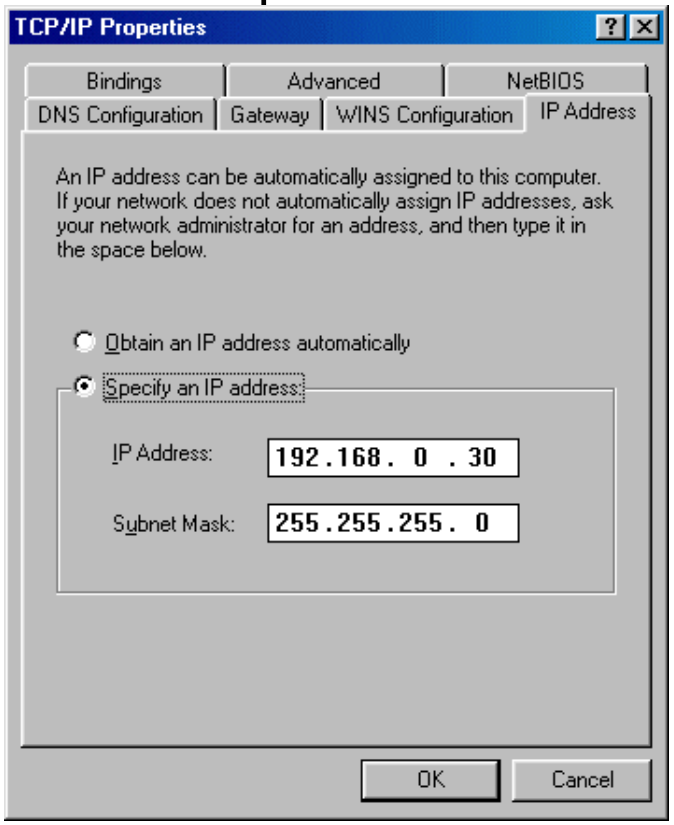
- Static
- Dynamic



# Static IP Addressing



- You have to go to each individual device
  - Meticulous records must be kept
  - No duplicate IP addresses



# Dynamic Addressing



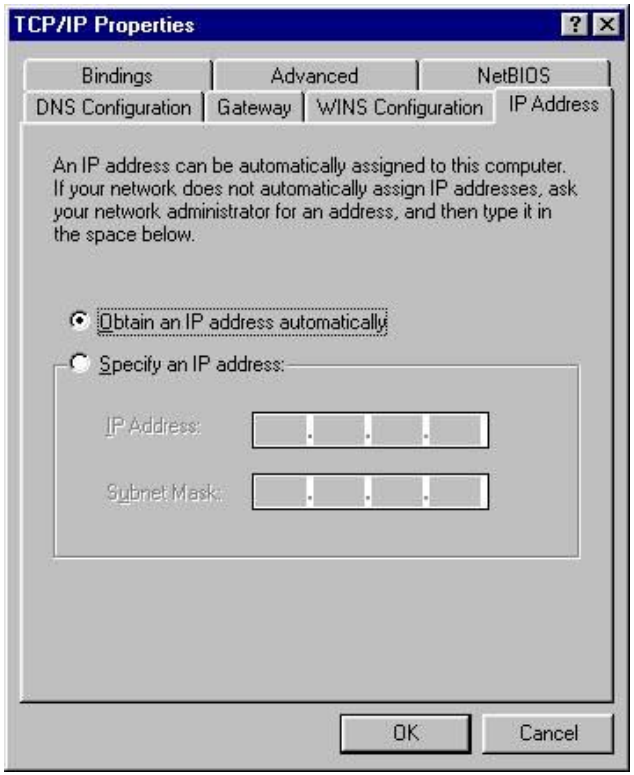
## Current Technology

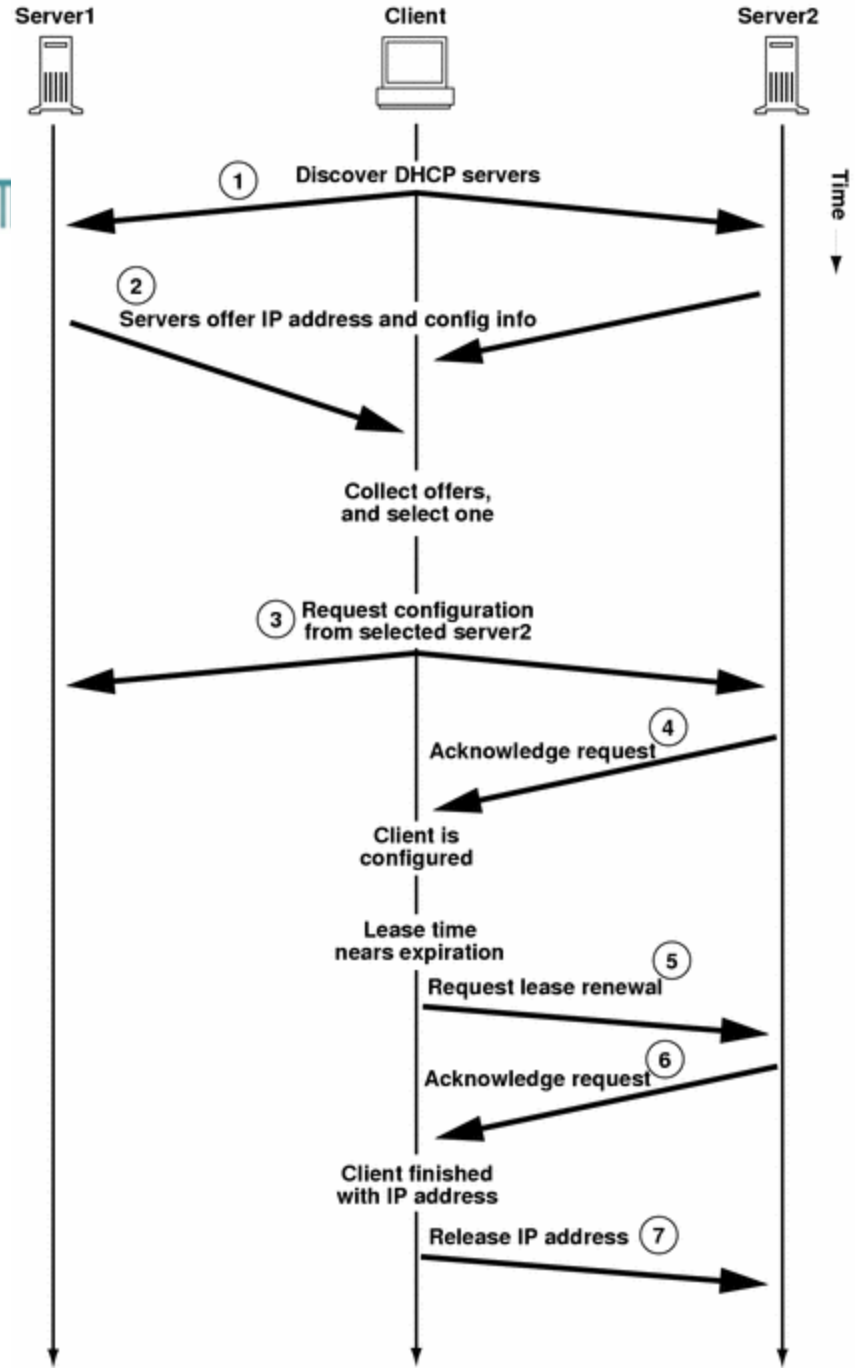
- **Dynamic Host Configuration Protocol (DHCP)**
  - Successor to BOOTP
  - Allows host to obtain an IP address quickly and dynamically
  - Uses a defined range of IP address

## Legacy Technologies

- **Reverse Address Resolution Protocol (RARP)**
  - Binds MAC addresses to IP addresses
- **BOOTstrap Protocol (BOOTP)**
  - Uses UDP to carry messages
  - Uses broadcast IP datagram
  - MAC address pre-matched to IP address
  - Can contain additional information (default gateway)

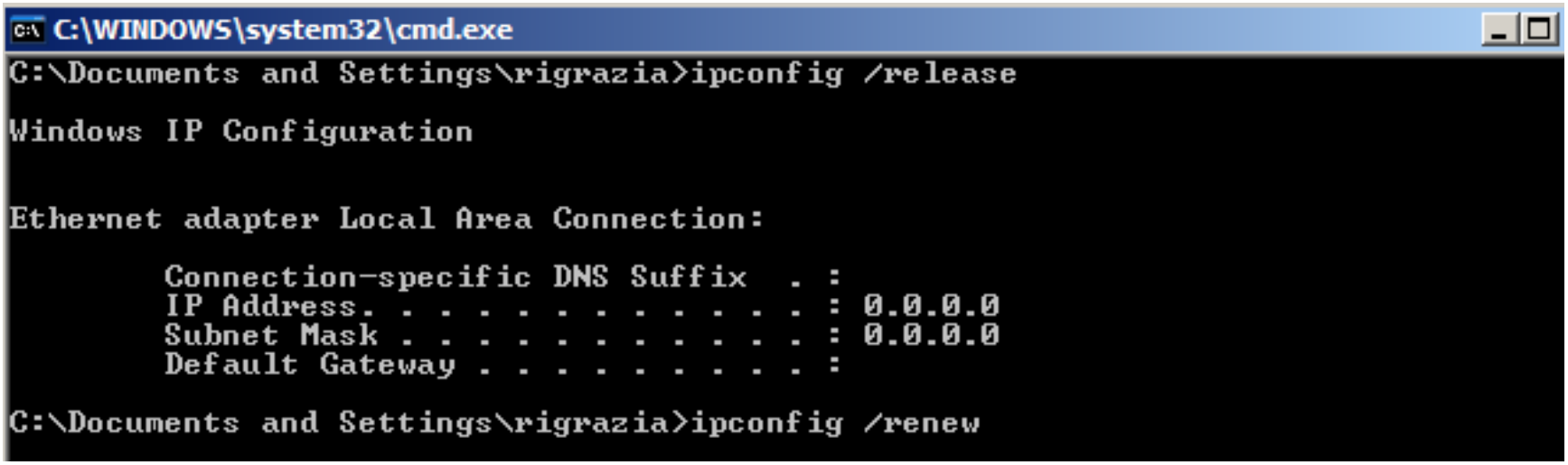
# DHCP


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel


Server1
Client
Server2
Time
1 Discover DHCP servers
2 Servers offer IP address and config info
Collect offers, and select one
3 Request configuration from selected server2
4 Acknowledge request
Client is configured
Lease time nears expiration
5 Request lease renewal
6 Acknowledge request
Client finished with IP address
Release IP address 7

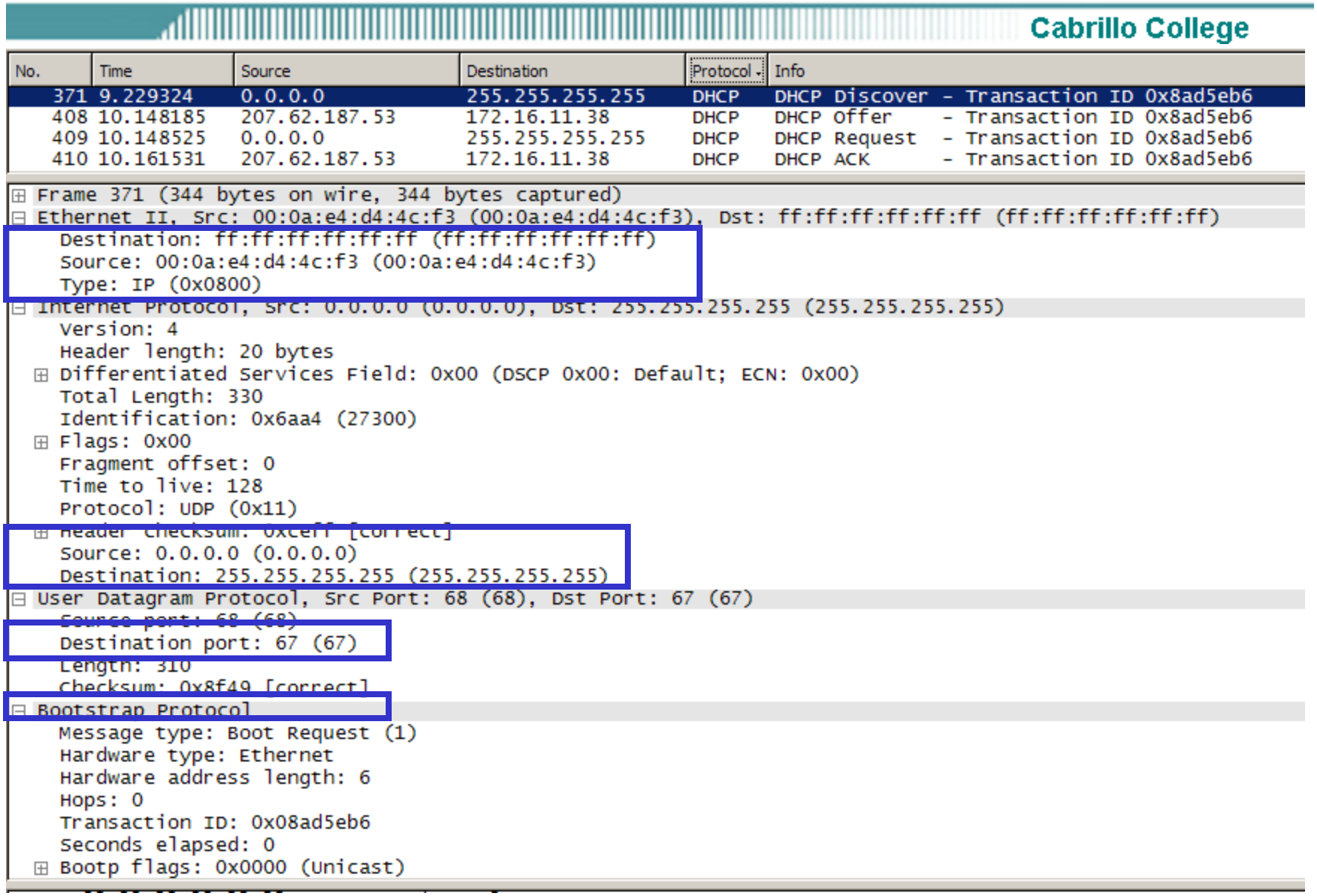
# Starting DHCP






- DHCP begins at startup or can be done with:
  - ipconfig /release
  - ipconfig /renew

# DHCP Discover: Host, “I need an IP Address…”

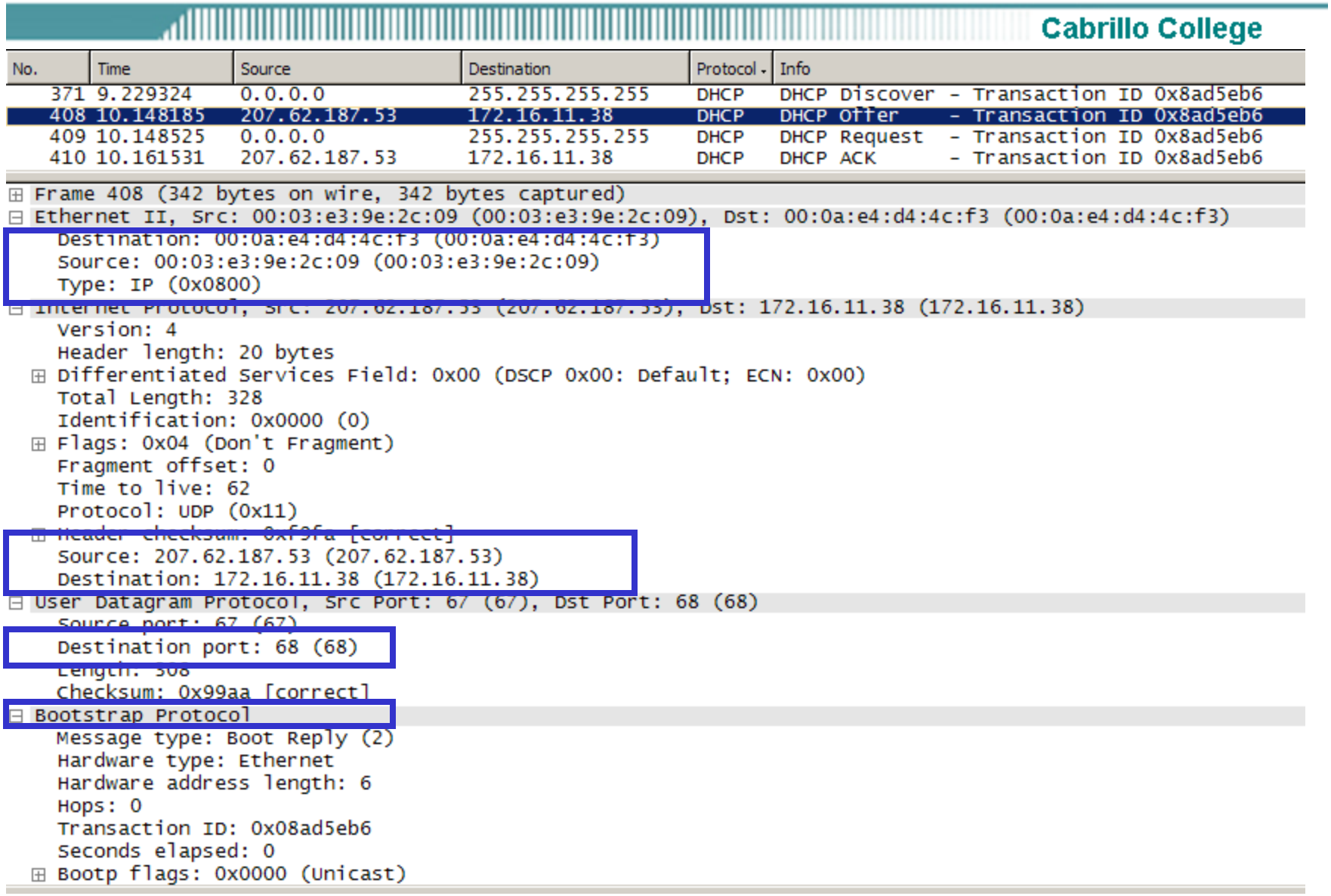


# DHCP Discover: Host, “I need an IP Address…”



```
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08ad5eb6
    Seconds elapsed: 0
  ⊟ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Discover
    Option 116: DHCP Auto-Configuration (1 bytes)
  ⊞ Option 61: Client identifier
    Option 50: Requested IP Address = 172.16.11.38
    Option 12: Host Name = "RickLaptop-2552"
    Option 60: Vendor class identifier = "MSFT 5.0"
  ⊞ Option 55: Parameter Request List
    End Option
```

# DHCP Offer: Server, “I’ll offer one to you.”

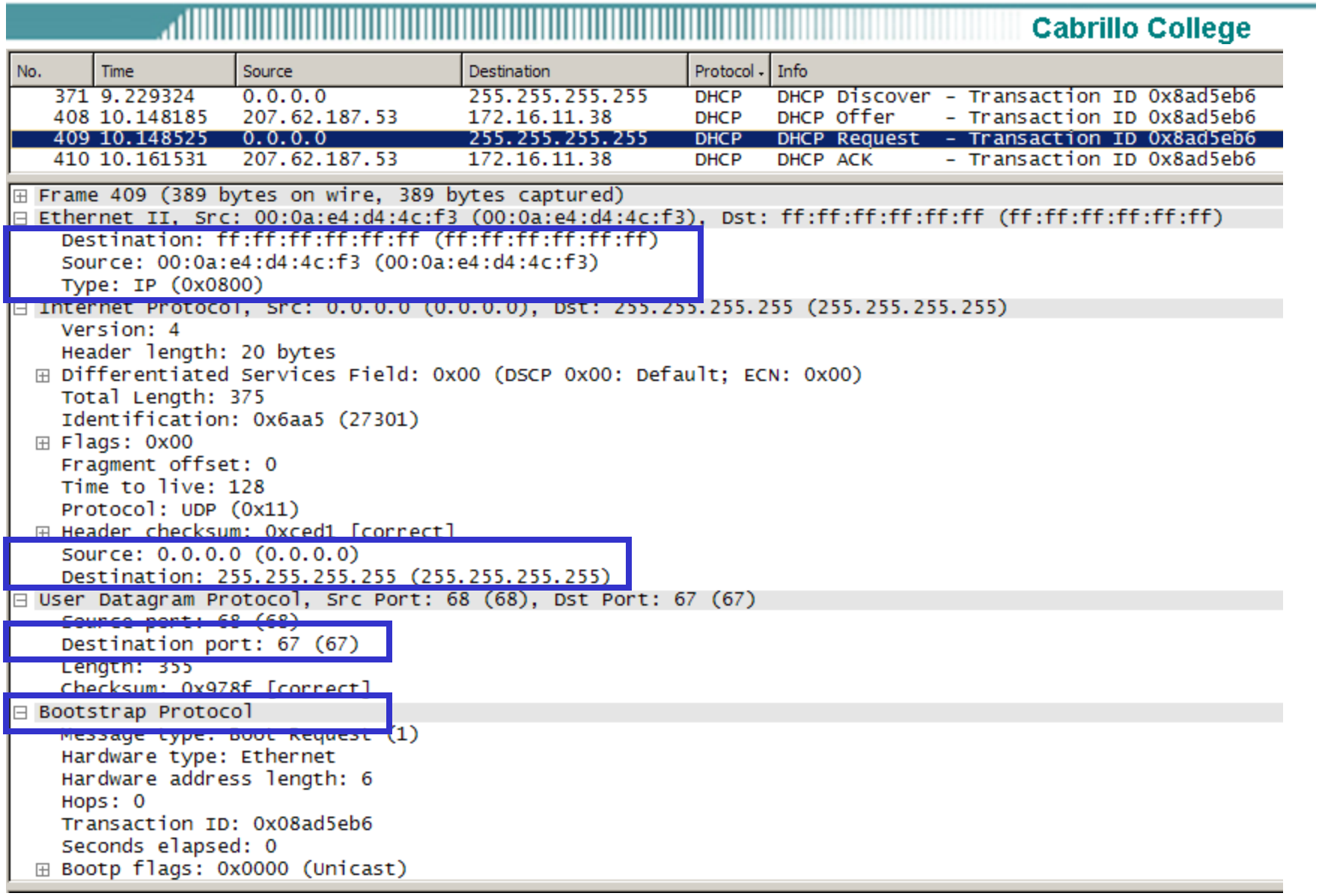


# DHCP Offer: Server, “I’ll offer one to you.”



```
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08ad5eb6
    Seconds elapsed: 0
  ⊟ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.16.11.38 (172.16.11.38)
    Next server IP address: 207.62.187.53 (207.62.187.53)
    Relay agent IP address: 172.16.0.1 (172.16.0.1)
    Client MAC address: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 54: Server Identifier = 207.62.187.53
    Option 51: IP Address Lease Time = 3 days
    Option 1: Subnet Mask = 255.255.224.0
    Option 15: Domain Name = "cabrillo.edu"
    Option 3: Router = 172.16.0.1
  ⊞ Option 6: Domain Name Server
    End Option
```

# DHCP Request: Host, “I’ll take it.”



# DHCP Request: Host, “I’ll take it.”



```
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08ad5eb6
    Seconds elapsed: 0
  ⊟ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
  ⊞ Option 61: Client identifier
    Option 50: Requested IP Address = 172.16.11.38
    Option 54: Server Identifier = 207.62.187.53
    Option 12: Host Name = "RickLaptop-2552"
  ⊞ Option 81: FQDN
    Option 60: Vendor class identifier = "MSFT 5.0"
  ⊞ Option 55: Parameter Request List
```

# DHCP ACK: Server, “It’s all yours.”

Cabrillo College

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 371 | 9.229324 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Discover - Transaction ID 0x8ad5eb6 |
| 408 | 10.148185 | 207.62.187.53 | 172.16.11.38 | DHCP | DHCP Offer - Transaction ID 0x8ad5eb6 |
| 409 | 10.148525 | 0.0.0.0 | 255.255.255.255 | DHCP | DHCP Request - Transaction ID 0x8ad5eb6 |
| 410 | 10.161531 | 207.62.187.53 | 172.16.11.38 | DHCP | DHCP ACK - Transaction ID 0x8ad5eb6 |

```
⊞ Frame 410 (362 bytes on wire, 362 bytes captured)
⊟ Ethernet II, Src: 00:03:e3:9e:2c:09 (00:03:e3:9e:2c:09), Dst: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Destination: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Source: 00:03:e3:9e:2c:09 (00:03:e3:9e:2c:09)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 207.62.187.53 (207.62.187.53), Dst: 172.16.11.38 (172.16.11.38)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 348
    Identification: 0x0000 (0)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 62
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xf9c6 [correct]
    Source: 207.62.187.53 (207.62.187.53)
    Destination: 172.16.11.38 (172.16.11.38)
⊟ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
    Source port: 67 (67)
    Destination port: 68 (68)
    Length: 328
    Checksum: 0xf616 [correct]
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08ad5eb6
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
```

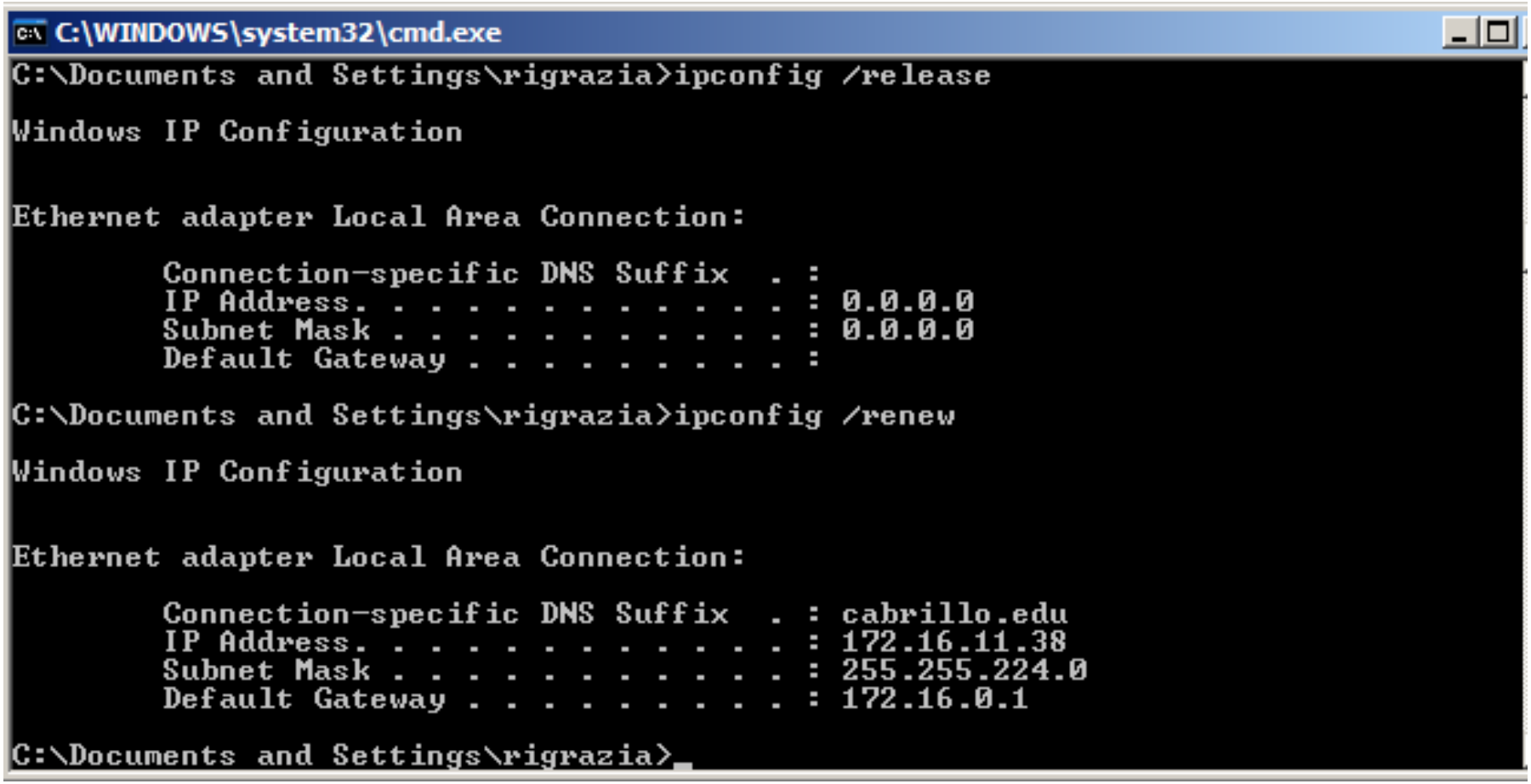
# DHCP ACK: Server, “It’s all yours.”



```
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x08ad5eb6
    Seconds elapsed: 0
  ⊟ Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.16.11.38 (172.16.11.38)
    Next server IP address: 207.62.187.53 (207.62.187.53)
    Relay agent IP address: 172.16.0.1 (172.16.0.1)
    Client MAC address: 00:0a:e4:d4:4c:f3 (00:0a:e4:d4:4c:f3)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 207.62.187.53
    Option 51: IP Address Lease Time = 3 days
  ⊞ Option 81: FQDN
    Option 1: Subnet Mask = 255.255.224.0
    Option 15: Domain Name = "cabrillo.edu"
    Option 3: Router = 172.16.0.1
  ⊞ Option 6: Domain Name Server
    End Option
```

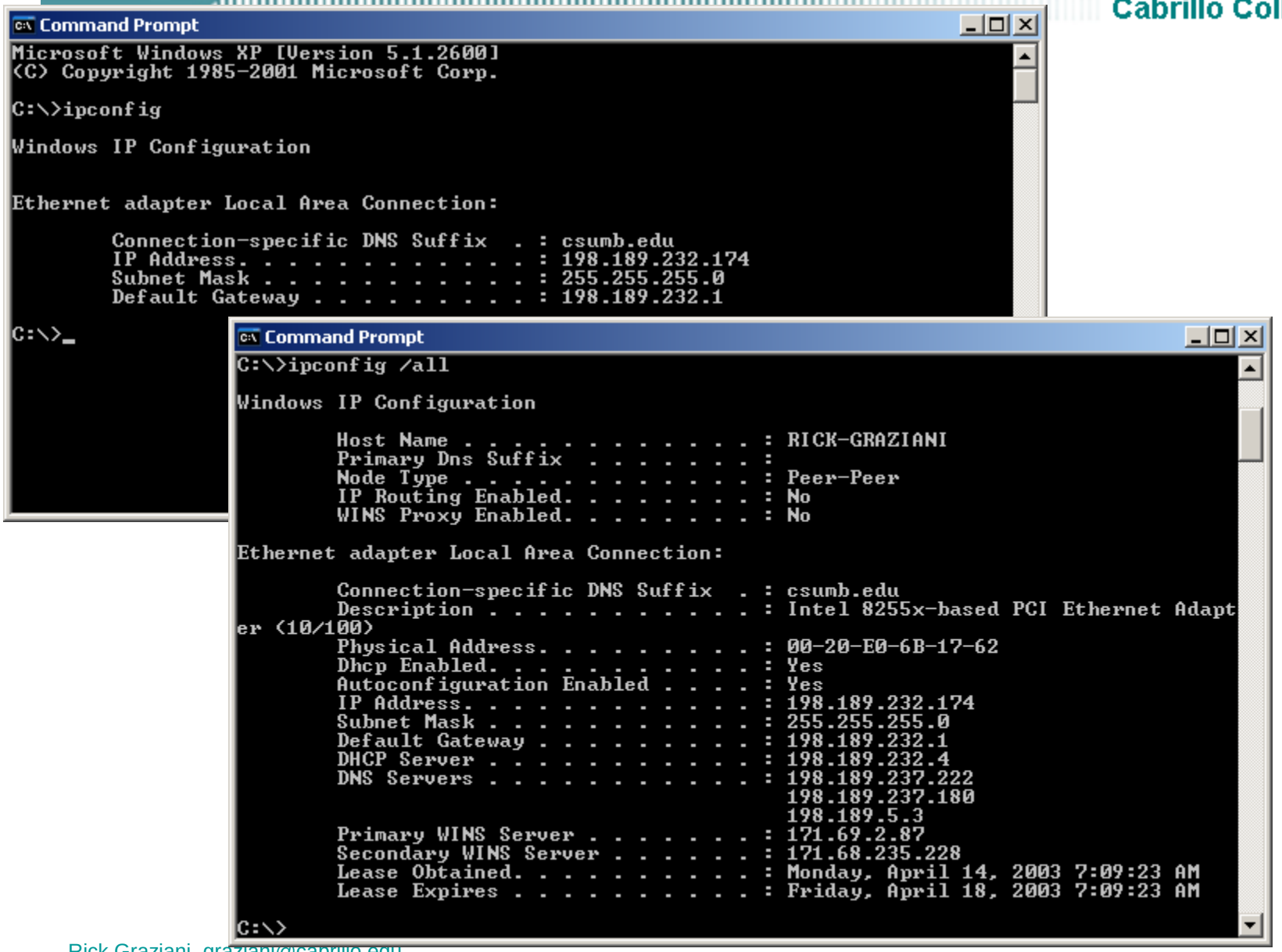
# The result…




C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\rigrazia>ipconfig /release
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
C:\Documents and Settings\rigrazia>ipconfig /renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : cabrillo.edu
IP Address. . . . . : 172.16.11.38
Subnet Mask . . . . . : 255.255.224.0
Default Gateway . . . . . : 172.16.0.1
C:\Documents and Settings\rigrazia>

# DHCP – Getting more than the IP Address





# From Microsoft: Conflict Detection



- Use server-side conflict detection on DHCP servers only when it is needed.
- Conflict detection can be used by either DHCP servers or clients to determine whether an IP address is already in use on the network before leasing or using the address.
- DHCP client computers running Windows 2000 or Windows XP that obtain an IP address use a gratuitous ARP request to perform client-based conflict detection before completing configuration and use of a server offered IP address. If the DHCP client detects a conflict, it will send a DHCP decline message (DHCPDECLINE) to the server.
- If your network includes legacy DHCP clients (clients running a version of Windows earlier than Windows 2000), you can use server-side conflict detection provided by the DHCP Server service under specific circumstances. For example, this feature might be useful during failure recovery when scopes are deleted and recreated. For more information, see DHCP Troubleshooting.
- By default, the DHCP service does not perform any conflict detection. To enable conflict detection, increase the number of ping attempts that the DHCP service performs for each address before leasing that address to a client. Note that for each additional conflict detection attempt that the DHCP service performs, additional seconds are added to the time needed to negotiate leases for DHCP clients.
- Typically, if DHCP server-side conflict detection is used, you should set the number of conflict detection attempts made by the server to use one or two pings at most. This provides the intended benefits of this feature without decreasing DHCP server performance.
- For more information, see Enable address conflict detection.
- http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/75cd0e1f-f464-40ea-ac88-2060e6769f33.mspx

# RARP



- RARP, or Reverse Address Resolution Protocol.
- Like ARP, used to map MAC address to IP addresses.
- Unlike ARP, used by devices to find their own IP address, not MAC address.
- What kind of device would not know its own IP address?
- Dumb terminals are diskless workstations.
- Diskless workstations have no permanent storage (like a hard drive) to store network configurations.
- Dumb terminals will know their own MAC address because it's burned in to the card, but they have to use RARP to find their IP.


**Dumb Terminals**

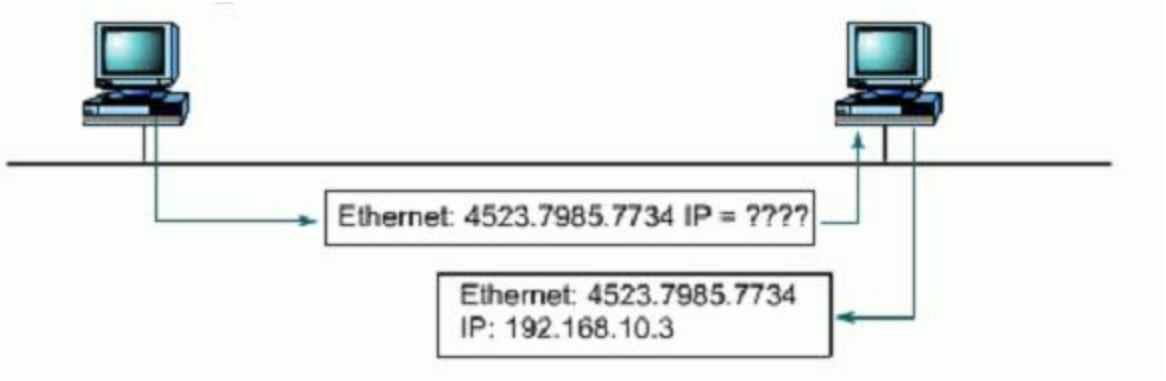
# RARP reply



- Only a RARP server can respond to a RARP request.
- RARP servers maintain a table of IP to MAC address mappings for RARP clients.
- During the boot process, RARP clients call the RARP server to obtain their IP configuration information.
- **Disadvantage**: RARP only returns an IP address, no subnet mask, default gateway, DNS address, etc.

**RARP Broadcast: I know my MAC address, but what is my IP address?**

**RARP Server Unicast: Here is your IP address.**



# BOOTP



**BOOTP (Bootstrap Protocol)**

- Provides IP address, subnet mask, default gateway IP address and DNS IP address.

**Disadvantage**:

- BOOTP is not a dynamic configuration protocol (like DHCP).
- When a client requests an IP address the BOOTP server looks up its MAC address in a table to find the IP address.
- This binding is predetermined.
- What if the computer is moved to another subnet/network?
- Use DHCP!

# ARP and Proxy ARP

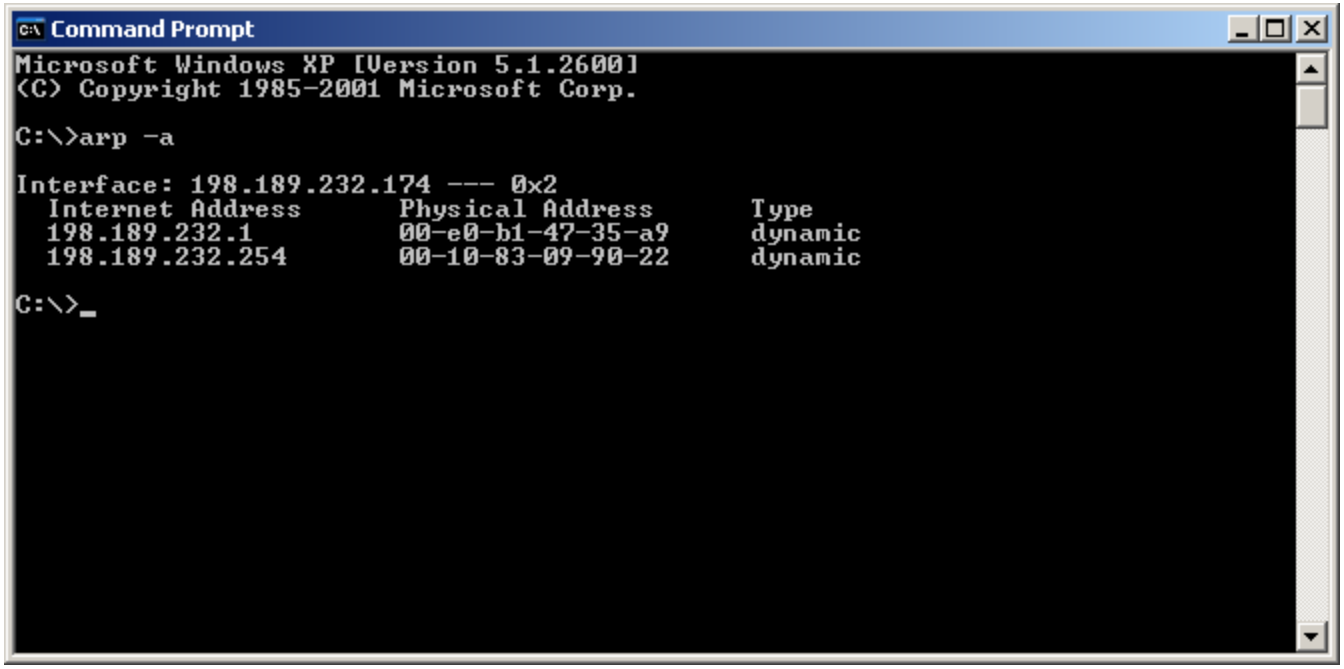


- See my PowerPoint presentation regarding ARP

# The ARP Table



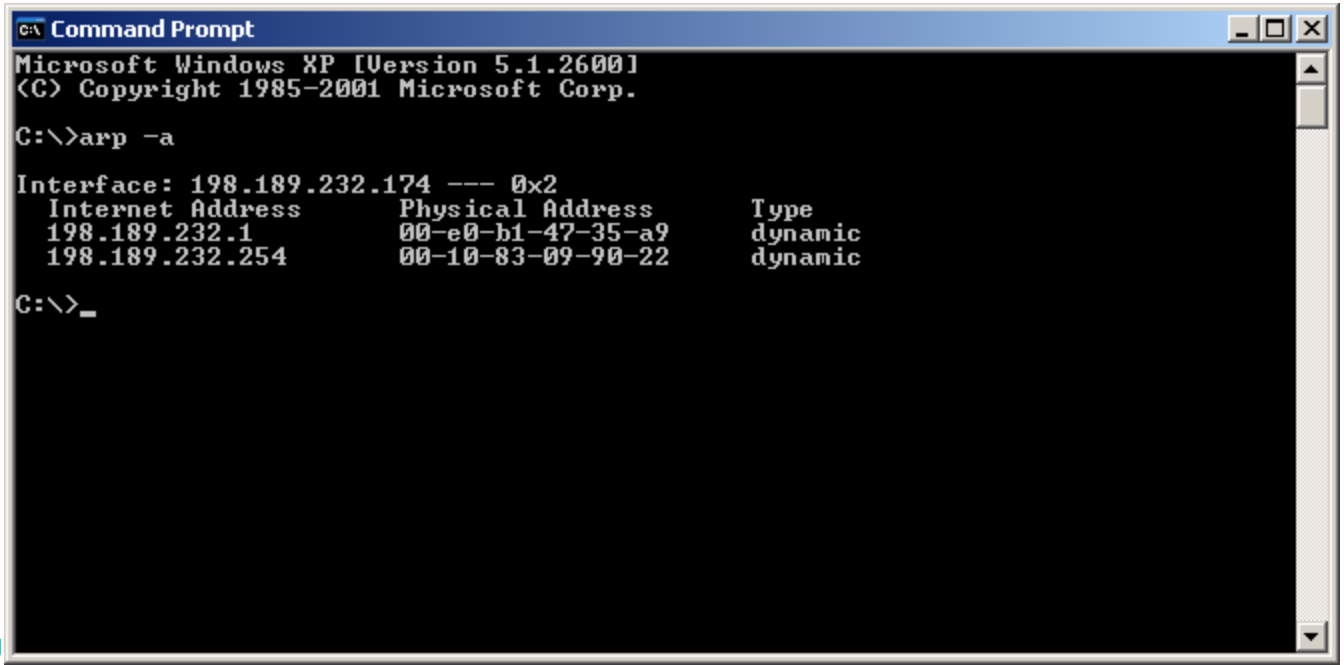
- The ARP table is stored in area of Random-Access Memory on each host.
- Such an area of memory is often called a cache. The ARP table is often referred to as an ARP cache.
- Entries in the ARP table “age out.” They are removed from the table after a period of inactivity.



# Aging Out



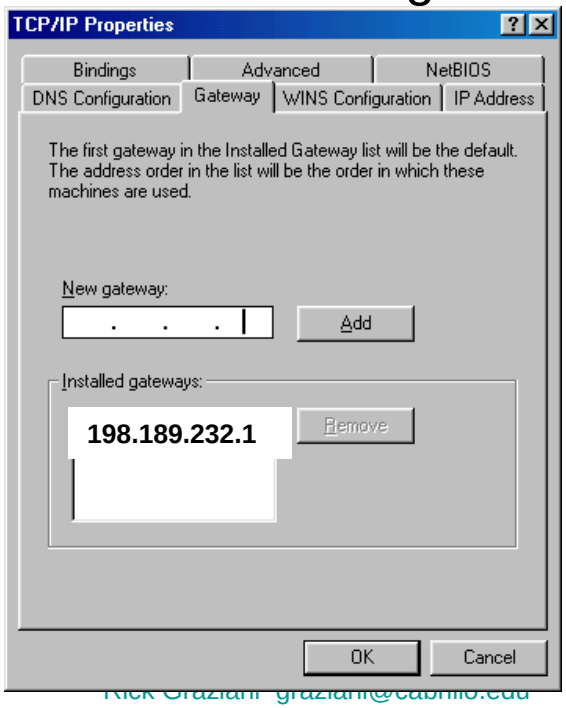
- For Microsoft Windows hosts:
  - Initial mappings have a 2-minute time-to-live.
  - An entry that is used twice in 2 minutes is automatically given a 10-minute time-to-live.
- For Unix/Linux hosts:
  - Initial mappings have a 20 minute time-to-live.

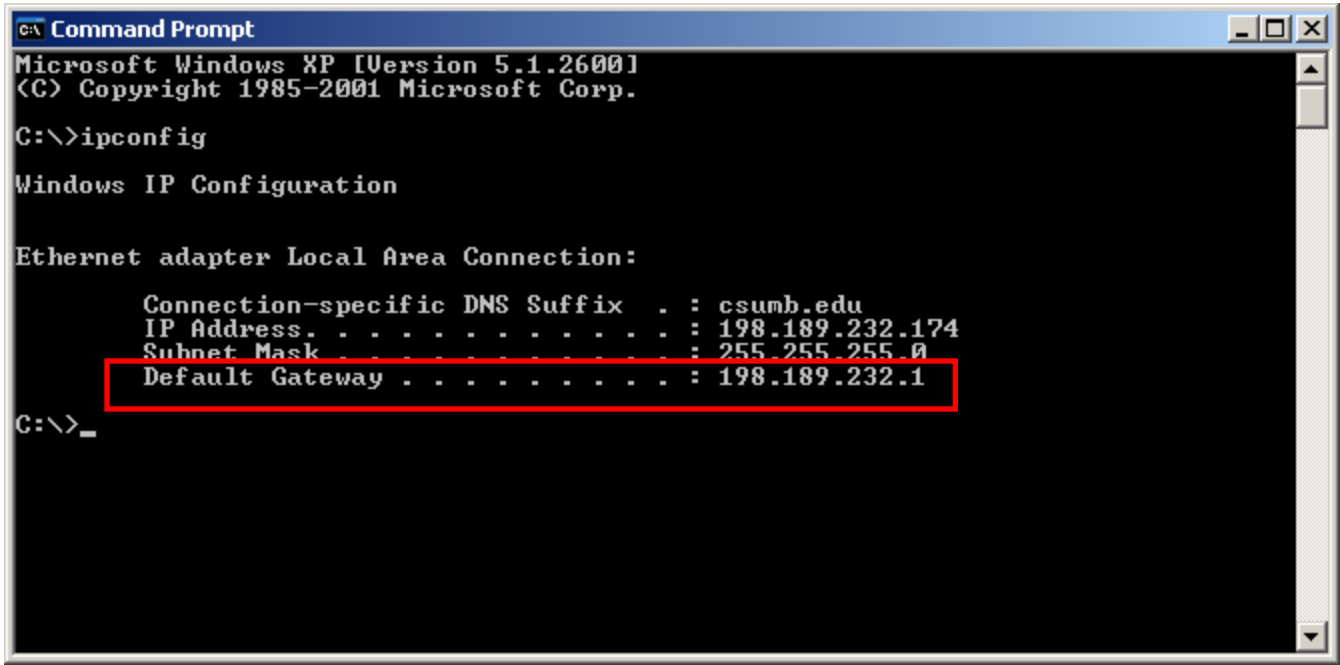


# Using a default gateway



- If the destination IP address is not on the same subnet (or network), a computer must use the services of a *router*.
- Routers are sometimes called *gateways* for this reason.
- Sending computer checks for a default gateway in its TCP/IP configuration.
- If no default gateway is installed, the sending computer cannot send the message.

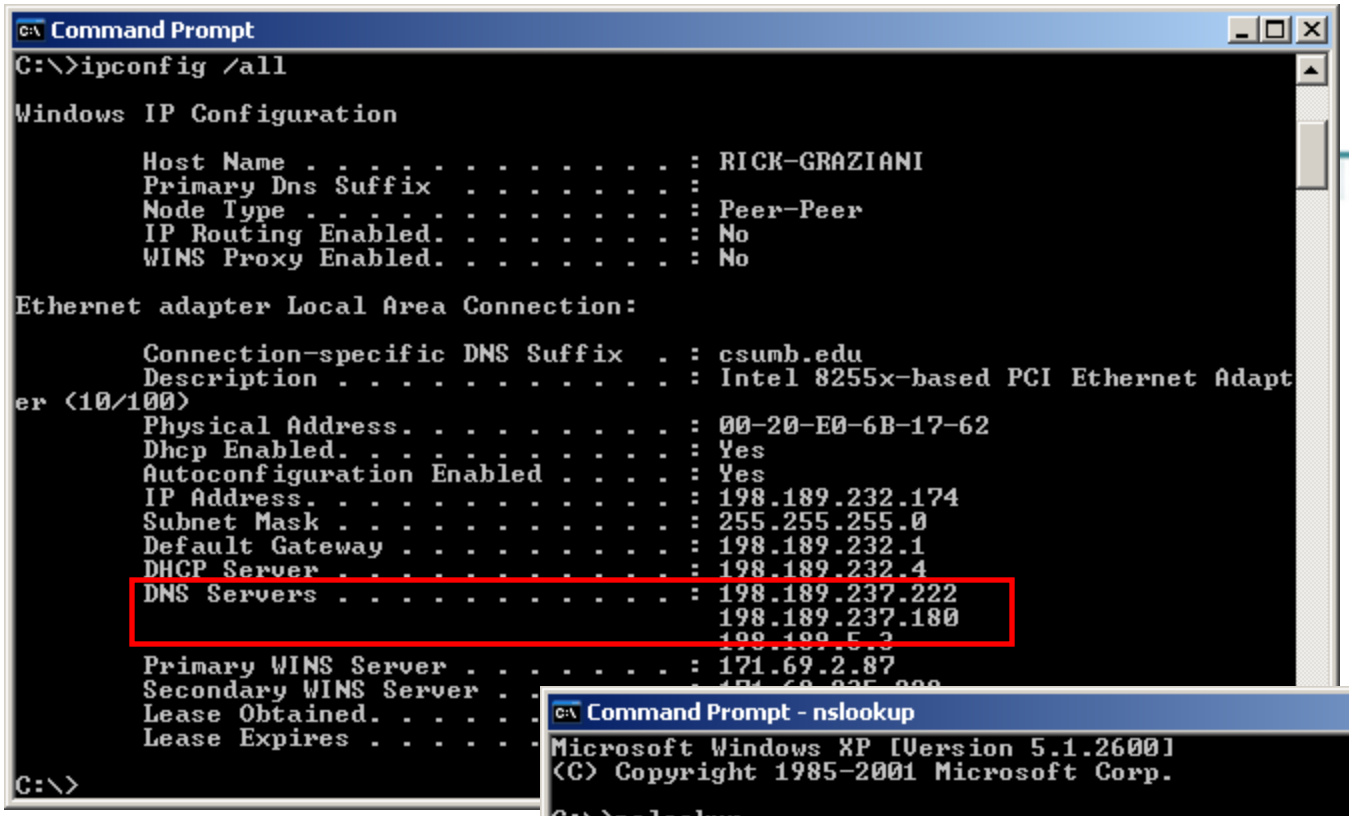


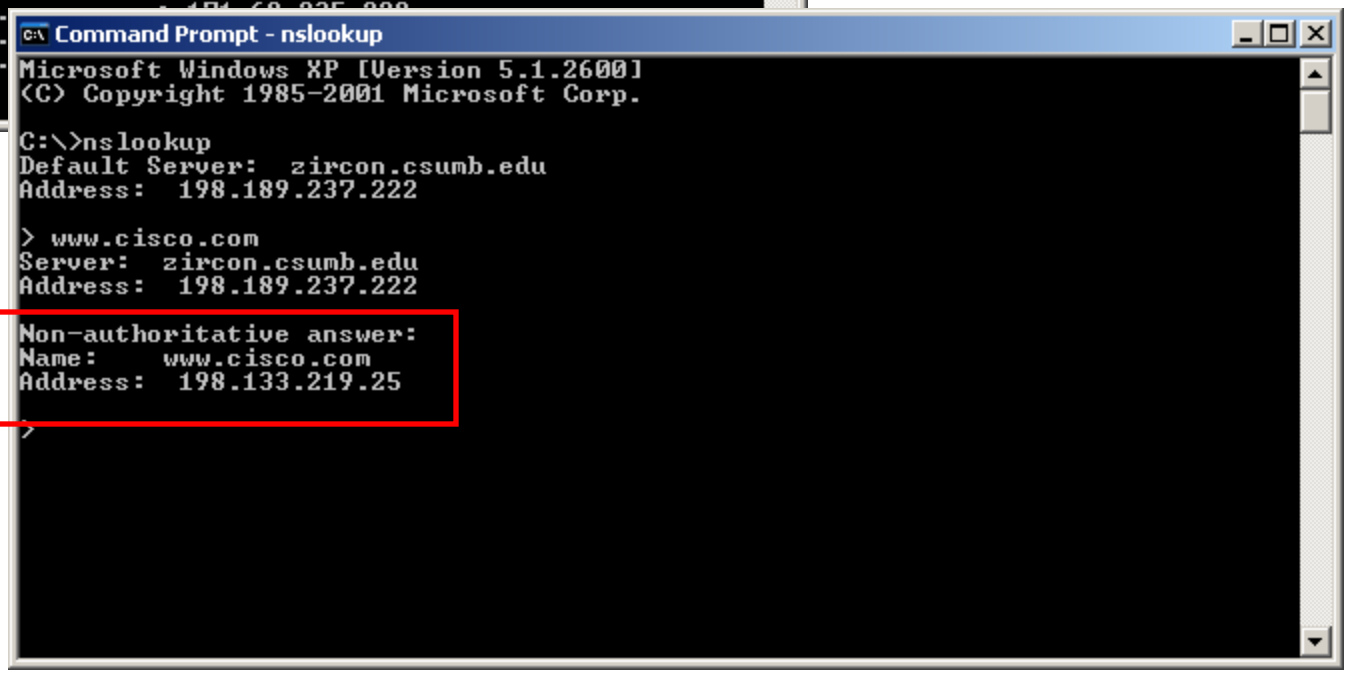



# Domain Names and IP Addresses



- Many times we communicate with other hosts using domain names such as **www.cisco.com**
- Hosts and routers route packets using IP addresses, NOT domain names.
- The host must translate the domain name to an IP address.
- The host will have the **DNS Server** do this translation for it.
- The **Domain Name System** (abbreviated DNS) is an Internet directory service.
- DNS is how domain names are translated into IP addresses, and DNS also controls email delivery.
- If your computer cannot access DNS, your web browser will not be able to find web sites, and you will not be able to receive or send email.

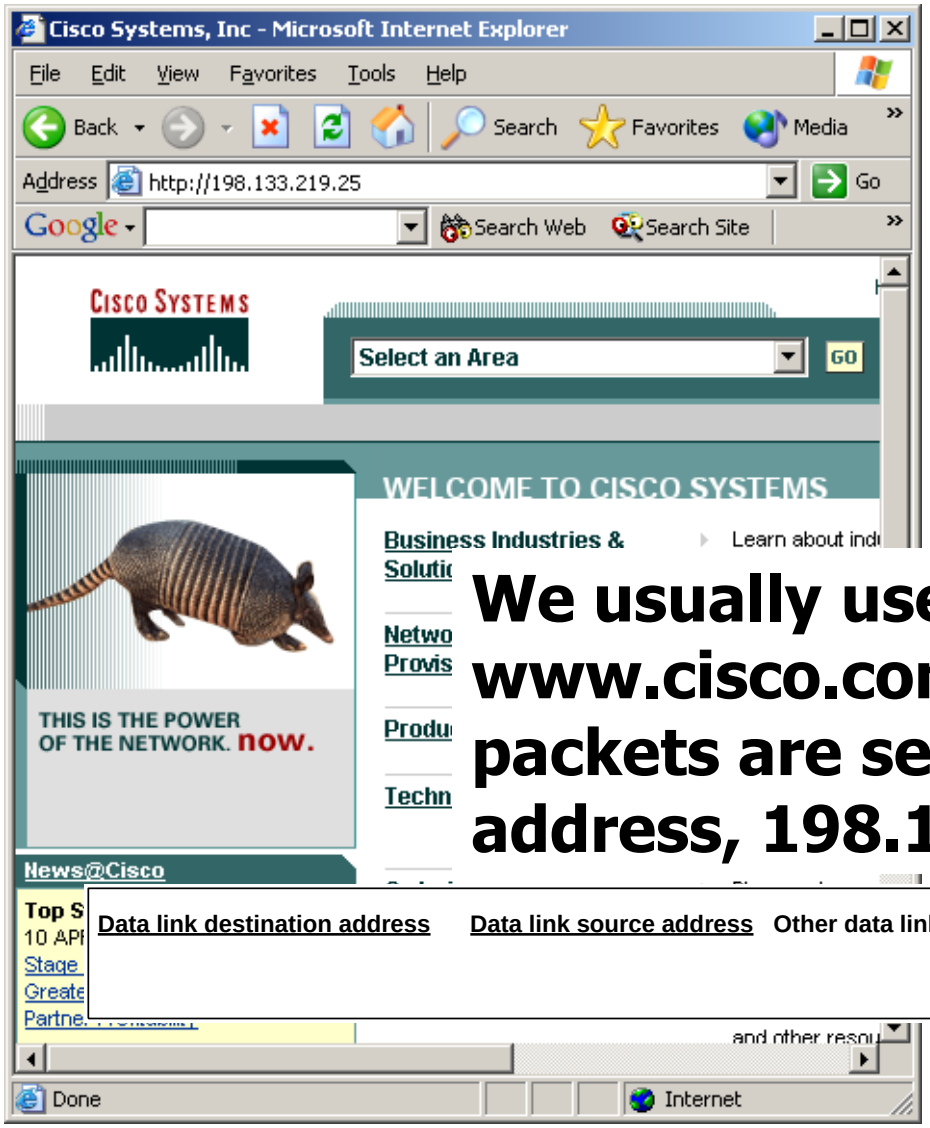


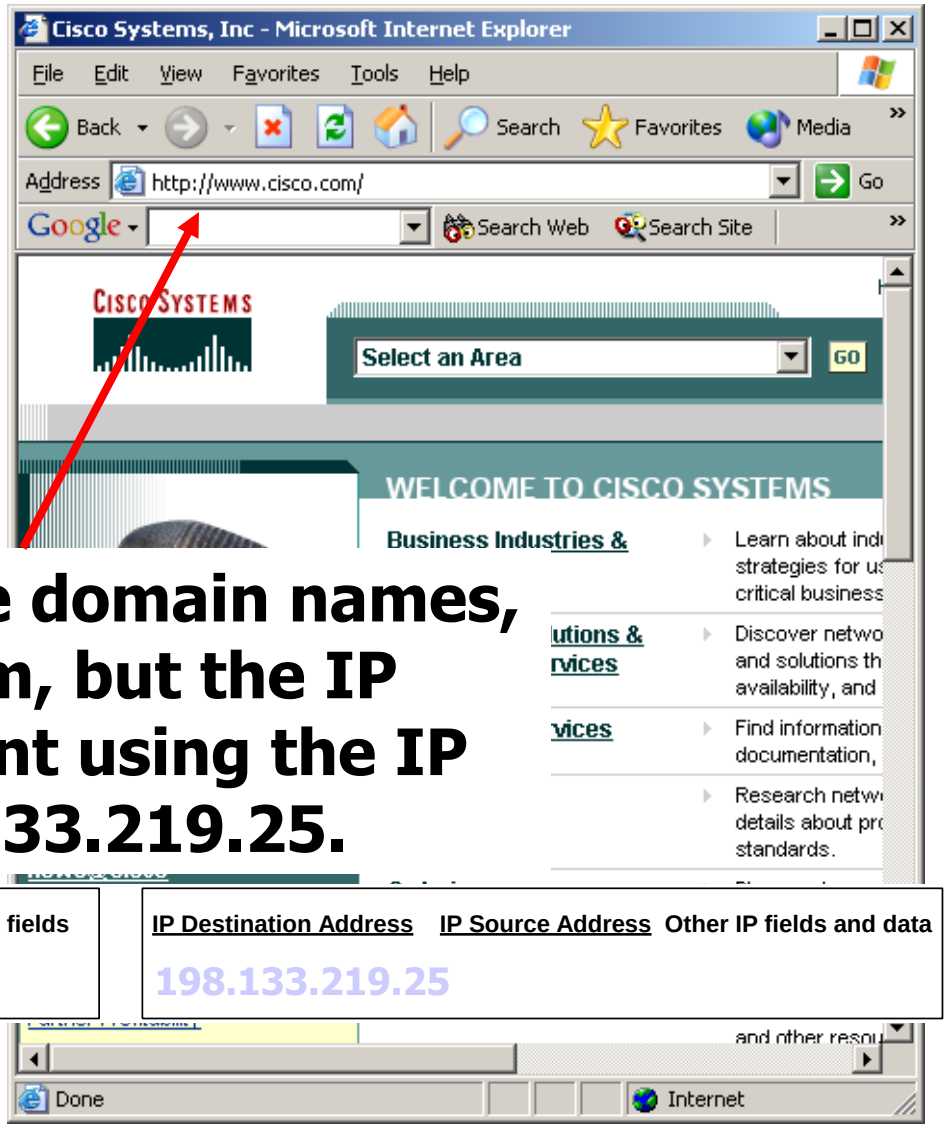




Cabrillo College

# Domain Names and IP Addresses






**We usually use domain names, www.cisco.com, but the IP packets are sent using the IP address, 198.133.219.25.**

| Data link destination address | Data link source address | Other data link fields |
|---|---|---|

| IP Destination Address | IP Source Address | Other IP fields and data |
|---|---|---|
| 198.133.219.25 | | |

# Name Resolution

# Name Resolution



- http://www.microsoft.com/technet/itsolutions/network/evaluate/technol/tcpipfund/tcpipfund_ch08.mspx

**Resolver**

- DNS client programs used to look up DNS name information.

**Name Resolution**

- The two types of queries that a DNS resolver (either a DNS client or another DNS server) can make to a DNS server are the following:

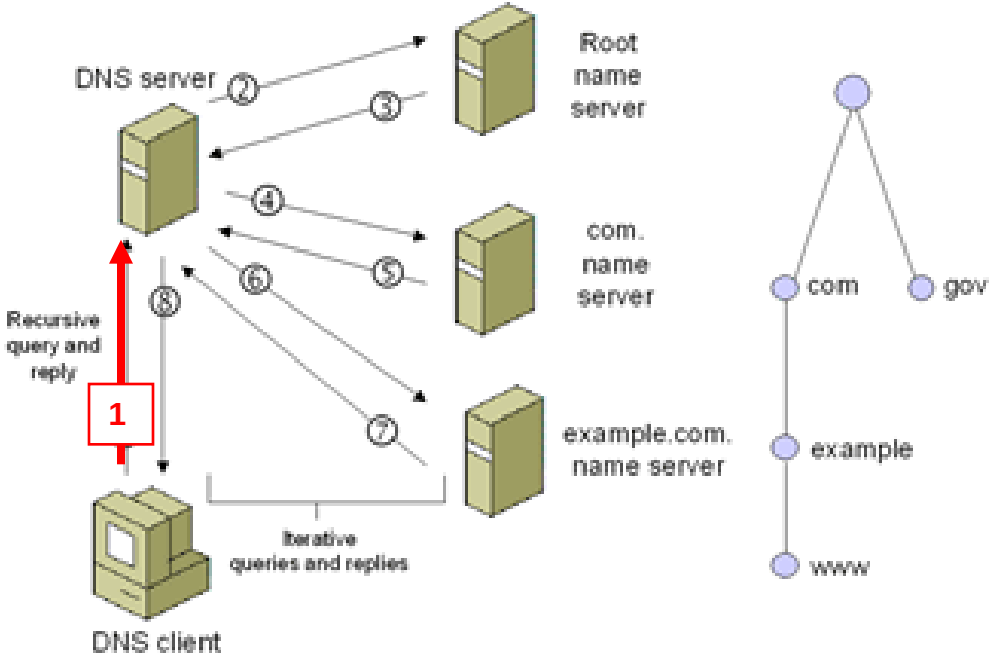
**Recursive queries**

- In a recursive query, the queried name server is requested to respond with the requested data or with an error stating that data of the requested type or the specified domain name does not exist.
- The name server cannot just refer the DNS resolver to a different name server.
- A **DNS client** typically sends this type of query.

**Iterative queries**

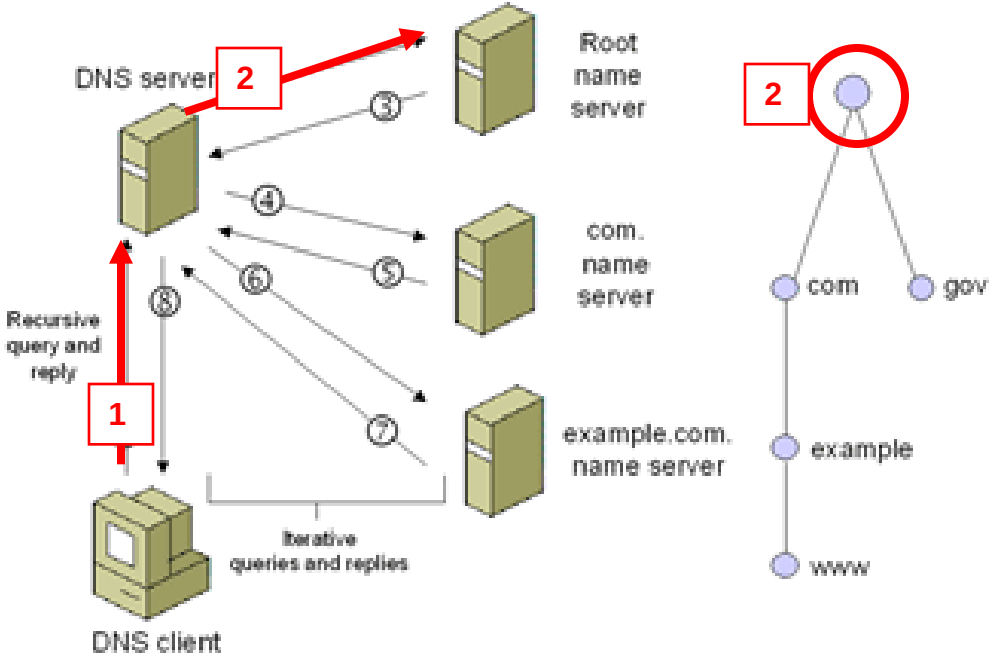
- In an iterative query, the queried name server can return the best answer it currently has back to the DNS resolver.
- The best answer might be the resolved name or a referral to another name server that is closer to fulfilling the DNS client's original request.
- **DNS servers** typically send iterative queries to query other DNS servers.

# DNS Name Resolution Example

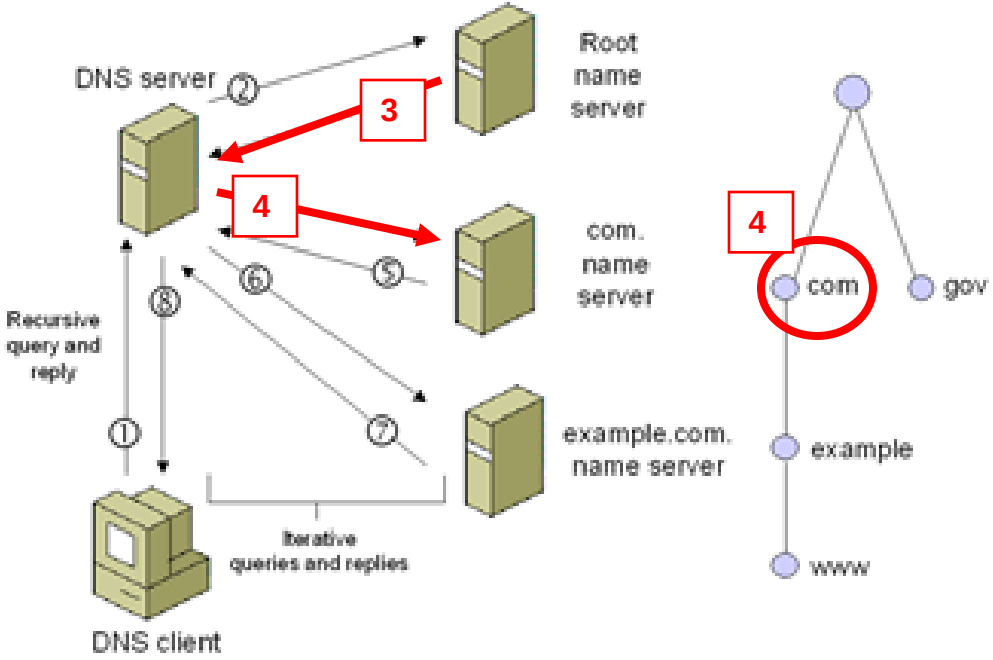

- To show how recursive and iterative queries are used for common DNS name resolutions, consider a computer running a Microsoft Windows® XP operating system or Windows Server 2003 connected to the Internet.
- A user types **http://www.example.com** in the Address field of their Internet browser.
- When the user presses the ENTER key, the browser makes a Windows Sockets function call, either *gethostbyname*() or *getaddrinfo*(), to resolve the name http://www.example.com to an IP address.
- For the DNS portion of the Windows host name resolution process, the following occurs:

# DNS Name Resolution Example

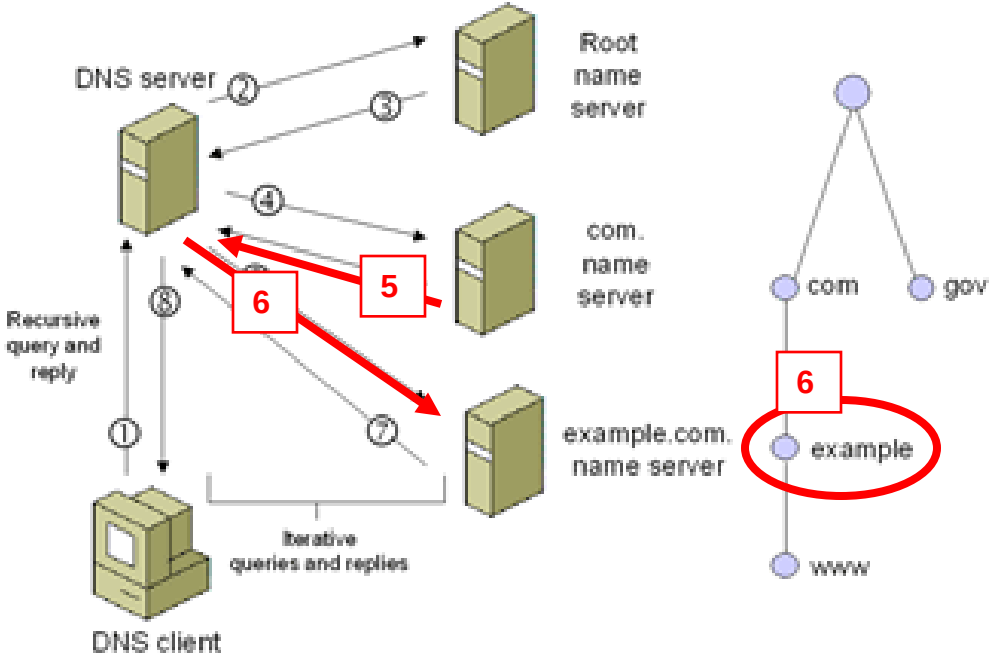

- 1.The **DNS resolver** on the **DNS client** sends a recursive query to its configured **DNS server**, **requesting the IP address corresponding to the name "www.example.com".**
  - The **DNS server for that client is responsible** for resolving the name and cannot refer the DNS client to another DNS server.
- 2.The **DNS server** that received the initial recursive query checks its zones and **finds no zones** corresponding to the requested domain name; the DNS server is **not authoritative for the example.com domain**.
  - Because the DNS server has no information about the IP addresses of DNS servers that are authoritative for example.com. or com., it **sends an iterative query for www.example.com. to a root name server.**

# DNS Name Resolution Example

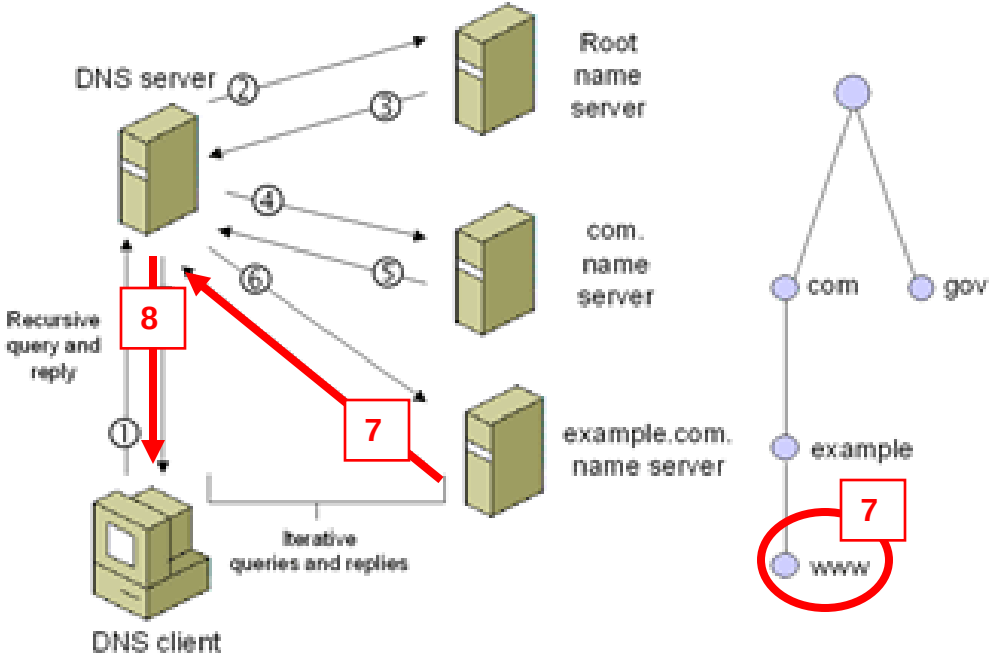

- 3.The **root name server** is authoritative for the root domain and has information about name servers that are authoritative for top-level domain names.
  - It is **not authoritative for the example.com. domain**.
  - Therefore, the **root name server replies with the IP address of a name server for the com. top-level domain**.
- 4.The **DNS server** of the DNS client sends an iterative query for www.example.com. **to the name server that is authoritative for the com.** top-level domain.

# DNS Name Resolution Example


- 5. **The com. name server** is **authoritative for the com. domain** and has information about the IP addresses of name servers that are authoritative for second-level domain names of the com. domain.
  - It is **not authoritative for the example.com. domain**.
  - Therefore, the **com. name server replies with the IP address of the name server that is authoritative for the example.com. domain.**
- 6.The **DNS server** of the DNS client sends an iterative query for www.example.com. **to the name server that is authoritative for the example.com. domain.**

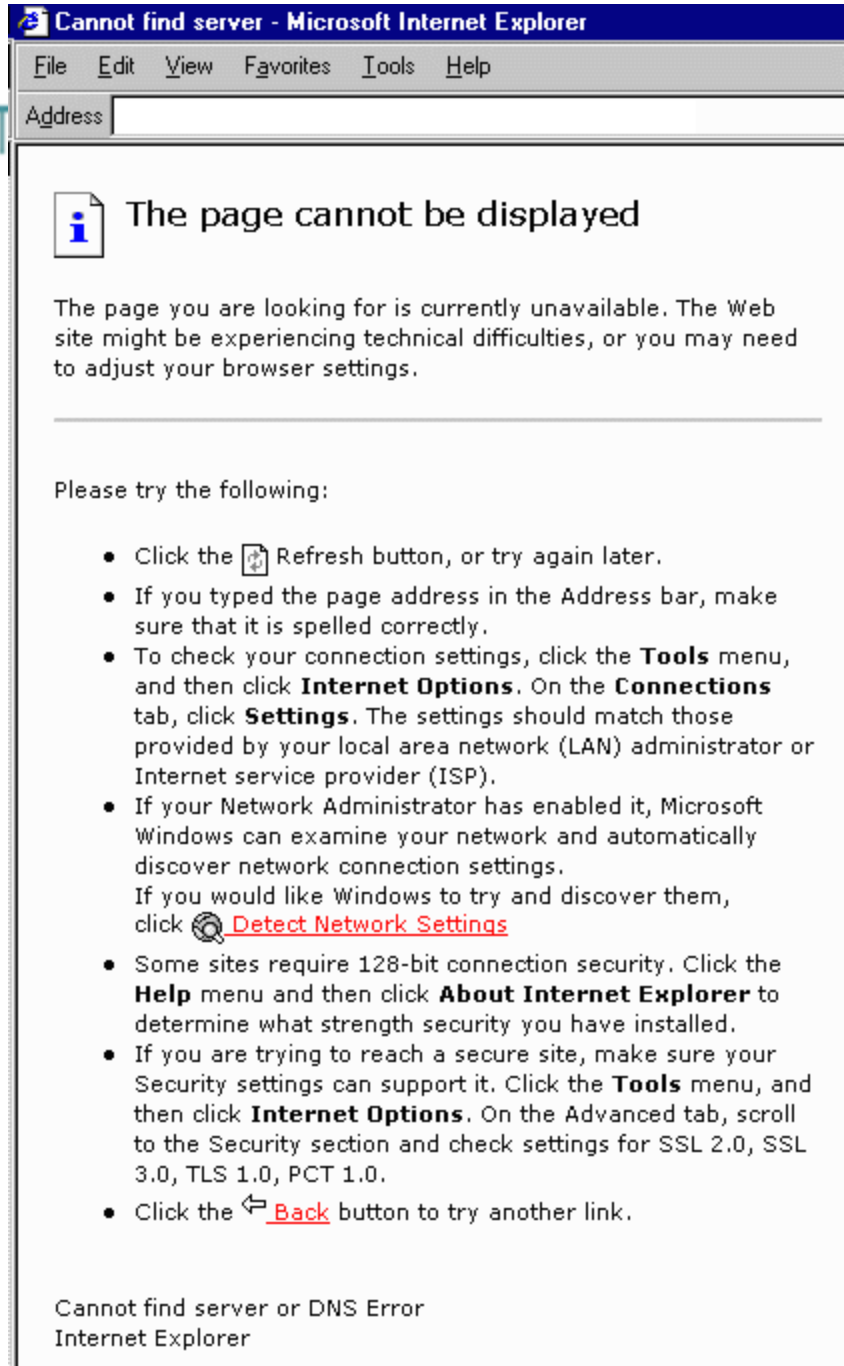
# DNS Name Resolution Example


- 7.**The example.com. name server replies with the IP address corresponding to the FQDN www.example.com.**
- 8.The **DNS server** of the DNS client **sends the IP address of www.example.com to the DNS client.**

# DNS Name Resolution Example

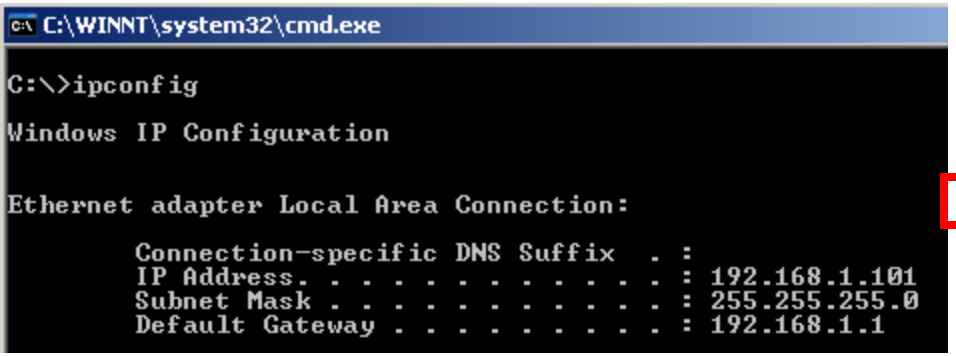
- In the worst cases, you'll get a dialog box that says the domain name doesn't exist - even though you know it does.
- This happens because the authoritative server is slow replying to the first, and your computer gets tired of waiting so it times-out (drops the connection) or the domain name does not exist.
- But if you try again, there's a good chance it will work, because the authoritative server has had enough time to reply, and your name server has stored the information in its cache.



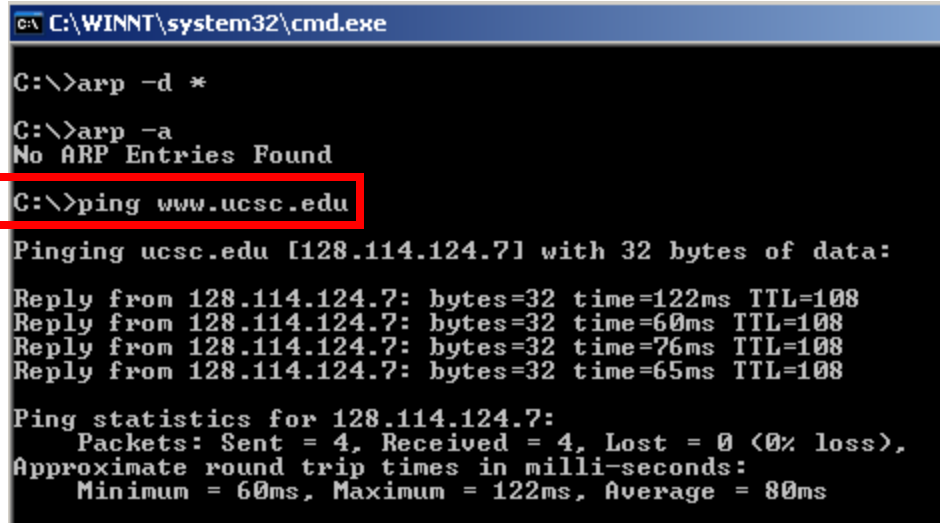
# DNS Name Resolution Example

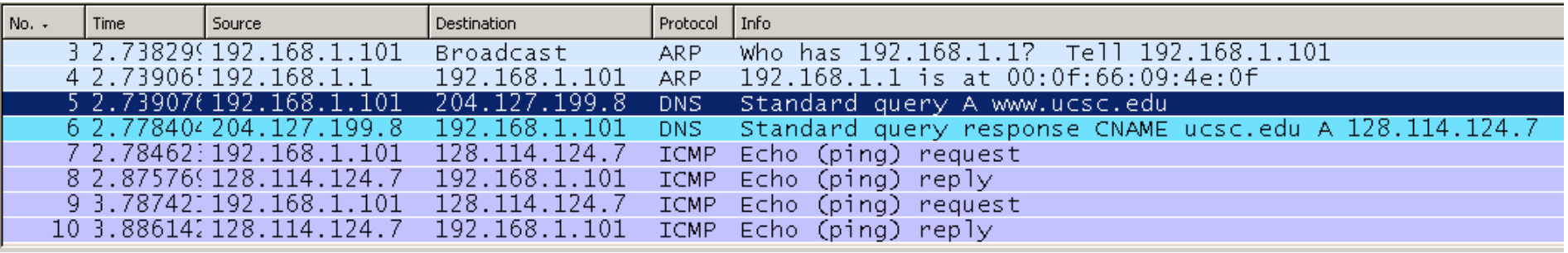


- **ipconfig /displaydns**
  - Ipconfig displays the contents of the DNS resolver cache, including the DNS resource records preloaded from the Hosts file as well as any recently queried names that were resolved by the system.
  - After a certain amount of time, specified in the Time to Live (TTL) associated with the DNS resource record, the resolver discards the record from the cache. You can also flush the cache manually. After you flush the cache, the computer must query DNS servers again for any DNS resource records previously resolved by the computer.
  - To flush the cache manually by using Ipconfig
- At the command prompt, type: **ipconfig /flushdns**
  - The local Hosts file is preloaded into the resolver's cache and reloaded into the cache whenever Hosts is updated.
- The default TTL for positive responses is 86,400 seconds (1 day).
- The default TTL for negative responses is 300 seconds.

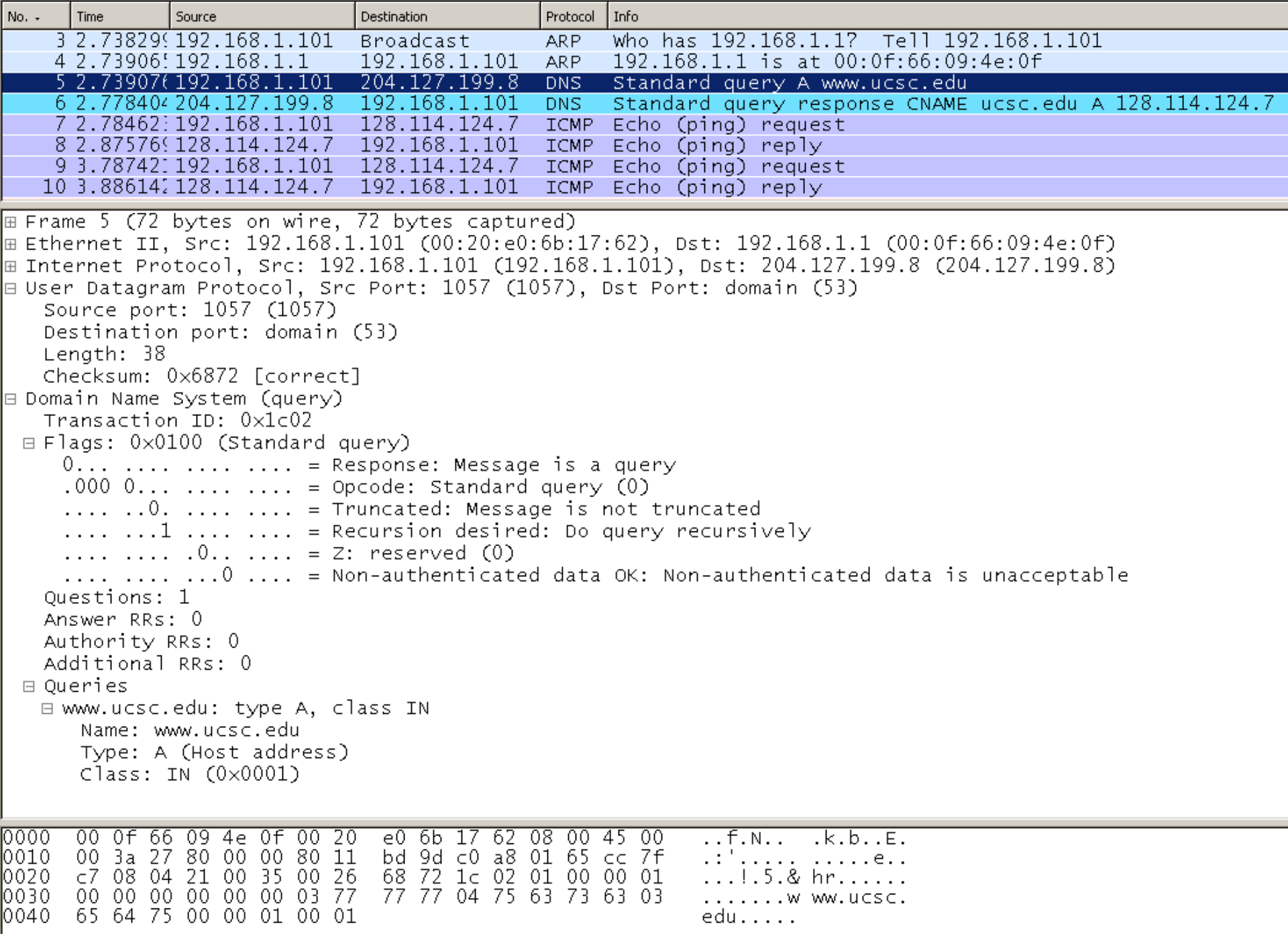


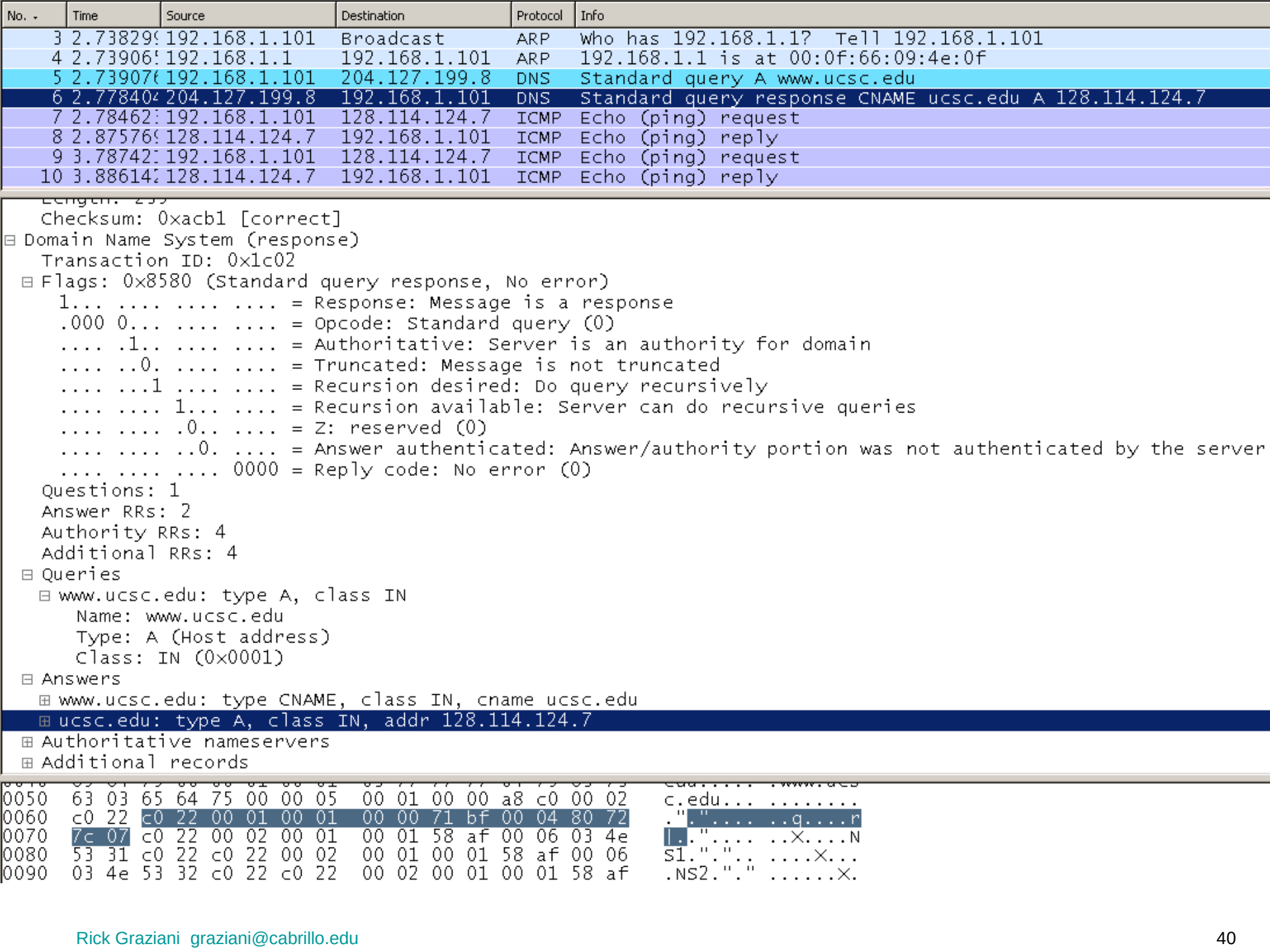

**(Missing Info) DNS: 204.127.199.8**

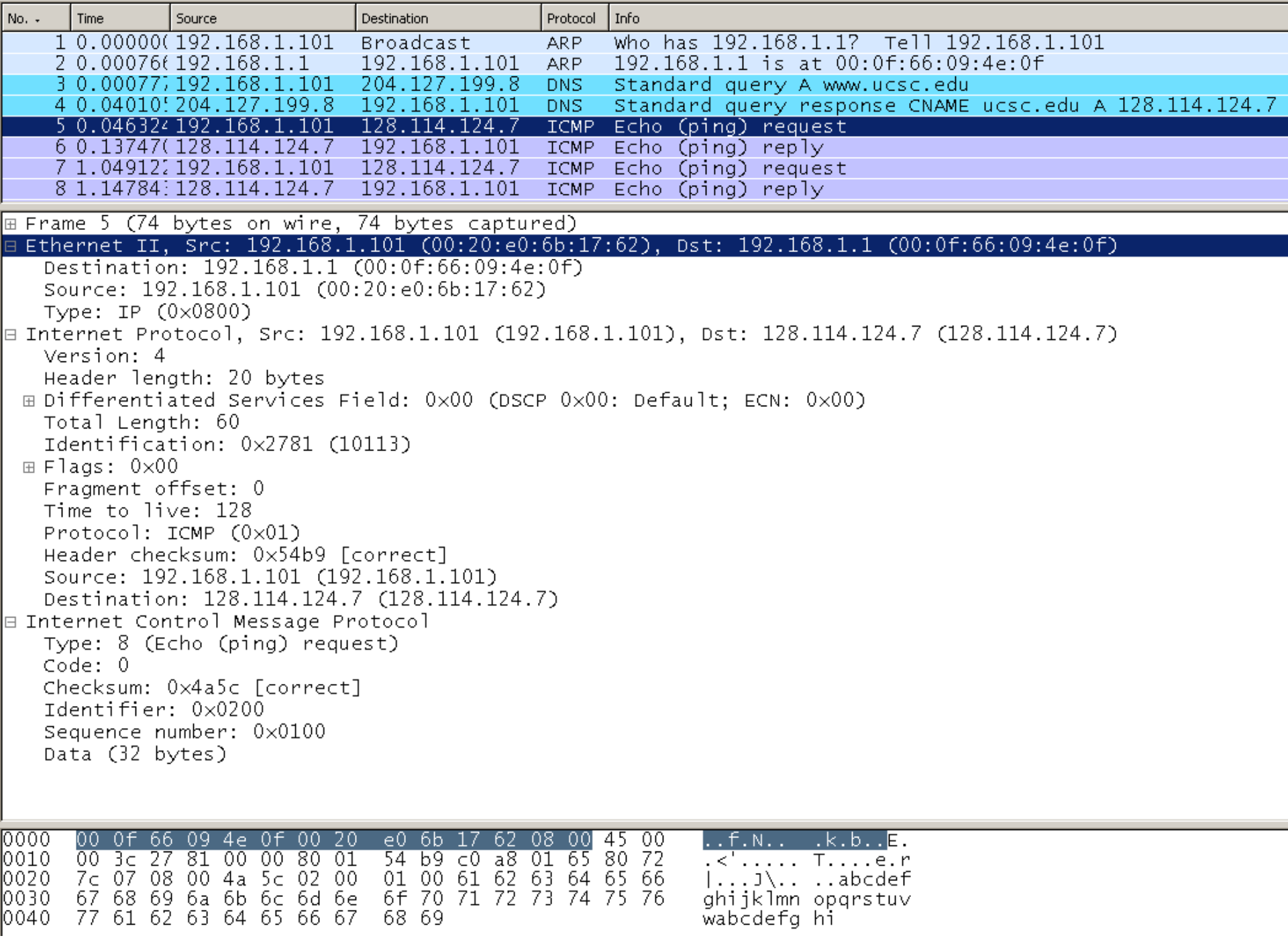



- So, why is the host issuing an ARP Request for the MAC Address of the Default Gateway (192.168.1.1)?
- Is it for the DNS Query or the ICMP Echo Request?
  - In this case it was for the DNS Query


No. Time Source Destination Protocol Info
3 2.73829 192.168.1.101 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.101
4 2.73906 192.168.1.1 192.168.1.101 ARP 192.168.1.1 is at 00:0f:66:09:4e:0f
5 2.73907 192.168.1.101 204.127.199.8 DNS Standard query A www.ucsc.edu
6 2.77840 204.127.199.8 192.168.1.101 DNS Standard query response CNAME ucsc.edu A 128.114.124.7
7 2.78462 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
8 2.87576 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
9 3.78742 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
10 3.88614 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
Frame 5 (72 bytes on wire, 72 bytes captured)
Ethernet II, Src: 192.168.1.101 (00:20:e0:6b:17:62), Dst: 192.168.1.1 (00:0f:66:09:4e:0f)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 204.127.199.8 (204.127.199.8)
User Datagram Protocol, Src Port: 1057 (1057), Dst Port: domain (53)
Source port: 1057 (1057)
Destination port: domain (53)
Length: 38
Checksum: 0x6872 [correct]
Domain Name System (query)
Transaction ID: 0x1c02
Flags: 0x0100 (Standard query)
0... .... .... .... = Response: Message is a query
.000 0... .... .... = Opcode: Standard query (0)
.... ..0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... .0.. .... = Z: reserved (0)
.... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ucsc.edu: type A, class IN
Name: www.ucsc.edu
Type: A (Host address)
Class: IN (0x0001)
0000 00 0f 66 09 4e 0f 00 20 e0 6b 17 62 08 00 45 00 ..f.N.. .k.b..E.
0010 00 3a 27 80 00 00 80 11 bd 9d c0 a8 01 65 cc 7f .:'..... .....e..
0020 c7 08 04 21 00 35 00 26 68 72 1c 02 01 00 00 01 ...!.5.& hr......
0030 00 00 00 00 00 00 03 77 77 77 04 75 63 73 63 03 .......w ww.ucsc.
0040 65 64 75 00 00 01 00 01 edu.....


No. Time Source Destination Protocol Info
3 2.73829 192.168.1.101 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.101
4 2.73906 192.168.1.1 192.168.1.101 ARP 192.168.1.1 is at 00:0f:66:09:4e:0f
5 2.73907 192.168.1.101 204.127.199.8 DNS Standard query A www.ucsc.edu
6 2.77840 204.127.199.8 192.168.1.101 DNS Standard query response CNAME ucsc.edu A 128.114.124.7
7 2.78462 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
8 2.87576 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
9 3.78742 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
10 3.88614 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
Checksum: 0xacb1 [correct]
Domain Name System (response)
Transaction ID: 0x1c02
Flags: 0x8580 (Standard query response, No error)
1... .... .... .... = Response: Message is a response
.000 0... .... .... = Opcode: Standard query (0)
.... .1.. .... .... = Authoritative: Server is an authority for domain
.... ..0. .... .... = Truncated: Message is not truncated
.... ...1 .... .... = Recursion desired: Do query recursively
.... .... 1... .... = Recursion available: Server can do recursive queries
.... .... .0.. .... = Z: reserved (0)
.... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
.... .... .... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 4
Additional RRs: 4
Queries
www.ucsc.edu: type A, class IN
Name: www.ucsc.edu
Type: A (Host address)
Class: IN (0x0001)
Answers
www.ucsc.edu: type CNAME, class IN, cname ucsc.edu
ucsc.edu: type A, class IN, addr 128.114.124.7
Authoritative nameservers
Additional records
0050 63 03 65 64 75 00 00 05 00 01 00 00 a8 c0 00 02
0060 c0 22 c0 22 00 01 00 01 00 00 71 bf 00 04 80 72
0070 7c 07 c0 22 00 02 00 01 00 01 58 af 00 06 03 4e
0080 53 31 c0 22 c0 22 00 02 00 01 00 01 58 af 00 06
0090 03 4e 53 32 c0 22 c0 22 00 02 00 01 00 01 58 af


No. Time Source Destination Protocol Info
1 0.00000( 192.168.1.101 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.101
2 0.00076( 192.168.1.1 192.168.1.101 ARP 192.168.1.1 is at 00:0f:66:09:4e:0f
3 0.00077; 192.168.1.101 204.127.199.8 DNS Standard query A www.ucsc.edu
4 0.04010! 204.127.199.8 192.168.1.101 DNS Standard query response CNAME ucsc.edu A 128.114.124.7
5 0.04632' 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
6 0.13747( 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
7 1.04912; 192.168.1.101 128.114.124.7 ICMP Echo (ping) request
8 1.14784: 128.114.124.7 192.168.1.101 ICMP Echo (ping) reply
Frame 5 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: 192.168.1.101 (00:20:e0:6b:17:62), Dst: 192.168.1.1 (00:0f:66:09:4e:0f)
Destination: 192.168.1.1 (00:0f:66:09:4e:0f)
Source: 192.168.1.101 (00:20:e0:6b:17:62)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.114.124.7 (128.114.124.7)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 60
Identification: 0x2781 (10113)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0x54b9 [correct]
Source: 192.168.1.101 (192.168.1.101)
Destination: 128.114.124.7 (128.114.124.7)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4a5c [correct]
Identifier: 0x0200
Sequence number: 0x0100
Data (32 bytes)
0000 00 0f 66 09 4e 0f 00 20 e0 6b 17 62 08 00 45 00 ..f.N.. .k.b..E.
0010 00 3c 27 81 00 00 80 01 54 b9 c0 a8 01 65 80 72 .<'..... T....e.r
0020 7c 07 08 00 4a 5c 02 00 01 00 61 62 63 64 65 66 |...J\.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

# IP Address Allocation, Resolution

Cabrillo College

CIS 81 and CST 311

Rick Graziani

Cabrillo College

Spring 2006